

FILED
TIME 2:57 PM

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

NOV 27 2017

RICHARD W. NAGEL
Clerk of Court
CINCINNATI, OHIO

IN THE MATTER OF THE SEARCH OF A
BLACK ZTE CELL PHONE AND A
SILVER LG CELL PHONE CURRENTLY
IN THE CUSTODY OF ATF

Case No. **1:17MJ-912**

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, JOHN SCOTT, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”), and have been since April 2000. During my time as a federal criminal investigator, I have participated in numerous investigations that have resulted in the execution of Federal search warrants. I am familiar with the Federal statutes pertaining to criminal use and possession of firearms as outlined in the 1968 Gun Control Act.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is (1) a black ZTE cell phone, model ZTE N817, serial number 325773808B2C; and (2) a silver LG cell phone, model LGMS210, serial number 701CYLH606808, hereinafter the “Devices.” The Devices are currently in the custody of ATF.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

1. On or about July 2, 2017, at approximately 3:04 AM, two individuals (“Individual-1” and “Individual-2”) were captured on surveillance video kicking in a glass door and making entry into a gun store (“Gun Store-1”) that is a Federal Firearms Licensee (“FFL”), located on Reading Road, Sharonville, Ohio. I have reviewed surveillance video from Gun Store-1, and from that review, I have learned, among other things, the following:

a. Individual-1 and Individual-2 were in the vicinity of Gun Store-1 for at least an hour before the forced entry.

b. Individual-1 and Individual-2 fled Gun Store-1 approximately three minutes after they forced entry.

2. I have spoken with law enforcement about the robbery of Gun Store-1, and reviewed reports, and from those conversations and that review, I have learned, among other things, the following:

a. The owner of Gun Store-1 told law enforcement, in substance and in part, that approximately 20 firearms were stolen.

3. While canvassing the area around Gun Store-1, law enforcement located leaves that appeared to have urine on them. The leaves were collected and tested by the Ohio Bureau of Criminal Investigation crime lab, which identified creatinine¹ on the leaves. A preliminary association was made between the creatinine and the DNA profile of Seronte NEWBY and Ronqueize HEAD.

4. On or about July 8, 2017, at approximately 3:04 AM, two individuals resembling Individual-1 and Individual-2 were captured by surveillance video attempting to enter a gun store ("Gun Store-2") that is an FFL, located on Hempstead Drive, Cincinnati, Ohio. I have reviewed surveillance video from Gun Store-2, and from that review, I have learned, among other things, that the individuals fled Gun Store-2 almost immediately after an alarm inside Gun Store-2 was activated.

5. On or about July 8, 2017, at approximately 4:39 AM, an alarm activated at an FFL gun store ("Gun Store-3") located on Dixie Highway, Florence, Kentucky.²

6. Law enforcement spoke with the owner of Gun Store-3, who told law enforcement, in substance and in part, that approximately 22 firearms were stolen.

7. On or about July 16, 2017, at approximately 5:45 AM, two individuals resembling Individual-1 and Individual-2 were captured by surveillance video breaking into an FFL gun store ("Gun Store-4") located on Tahlequah Trail, Springboro, Ohio.

¹ Creatinine is a human waste product from the blood that passes through the kidneys and is then eliminated through urine.

² I know from an internet search that Gun Store-2 is approximately 23 miles from Gun Store-3.

8. Law enforcement spoke with the owner of Gun Store-4, who told law enforcement, in substance and in part, that approximately 32 firearms were stolen.

9. Law enforcement obtained historical cell sites for the phone number associated with Seronte NEWBY. Analysis revealed that the phone number hit off towers in the vicinity of the gun stores around the times of the robberies. For instance, on or about July 8, 2017—the day of the attempted robbery of Gun Store-2 and successful robbery of Gun Store-3—the phone number hit off of a tower in the area Gun Store-2 approximately a half an hour after the attempted robbery, and hit off of a tower in the area of Gun Store-3 approximately 15 minutes after the robbery.

10. On or about November 15, 2017, a Grand Jury in the Southern District of Ohio returned an indictment charging Seronte NEWBY and Ronqueize HEAD with, *inter alia*, conspiracy to commit theft of federal firearms licensees and theft of federal firearms licensees. On or about November 17, 2017, Seronte NEWBY and Ronqueize HEAD were arrested pursuant to arrest warrants.

11. The Devices are currently in the lawful possession of ATF. They came into ATF's possession pursuant to the lawful arrest of Seronte NEWBY, when ATF recovered the Devices from his person.

12. The Devices are currently in storage with ATF. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of ATF.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <http://www.lg.com/us/cell-phones/lg-MS210-Metro-PCS-aristo> and <http://assurancewireless.virginmobileusa.com/userguides/assets/aw-ztequest.pdf>, I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to plan robberies or broker gun sales, the individual’s electronic device will generally serve as a storage medium for evidence of the crime. From my training and experience, I

believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

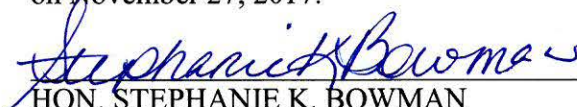
19. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



John Scott
Special Agent
Bureau of Alcohol, Tobacco, Firearms, and
Explosives

Subscribed and sworn to before me
on November 27, 2017:



HON. STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is (1) a black ZTE cell phone, model ZTE N817, serial number 325773808B2C; and (2) a silver LG cell phone, model LGMS210, serial number 701CYLH606808, hereinafter the “Devices.” The Devices are currently in the custody of ATF.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Sections 371 and 922(u) and involve SERONTE NEWBY since May 1, 2017, including:

- a. Evidence of planning and/or execution of firearm robberies, including purchase of items used in firearm robberies;
- b. Evidence of firearm trafficking;
- c. Lists of customers and related identifying information;
- d. Types, amounts, and prices of guns trafficked, as well as dates, places, and amounts of specific transactions;
- e. Any information related to sources of guns (including names, addresses, phone numbers, or any other identifying information);
- f. Schedule, travel, and location information;
- g. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.